UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/075,194	02/12/2002	Klimenty Vainstein	SSL1P003/SS-006	7090

22830 7590 07/14/2006

CARR & FERRELL LLP
2200 GENG ROAD
PALO ALTO, CA 94303

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/075,194	VAINSTEIN ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/7; 08/15*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 04/11/06. Applicant amended Claims 36, and 43. Applicants also have made an appropriate adjustment to Claims 43 to overcome claim objection as identified in previous office action. The amendment filed on 04/11/06 have been entered and made of record. Therefore, presently pending claims are 1-43.

Response to Arguments

Applicant's arguments filed 04/11/06 have been fully considered but they are not persuasive because of following reasons.

In reference to the support supplied in the specification for the limitations of claim 36, the applicant's arguments are not persuasive. The paragraphs 120 to 123 teach the authentication of the requestor by the central server and the local servers. However the specification does not teach the limitation "the given requestor can only access secured items through at most one of said local servers at a time." There is no written description for the controls of the devices such as the client controls the number of servers that it connects to or whether the central server discloses.

Applicant argued that a careful review of Stallings discloses that access control is not performed by the central server or the local servers. The applicant argues further that the central server and the local server are both required to perform access control and permit or deny access request to secure items by requestors. This is not found persuasive. In the Kerberos system the Central server performs the authentication process. Although it is true that the local server

performs an additional authentication, it is an additional authentication, not the initial authentication of the Central server as disclosed, by Stallings, in the Kerberos process. The initial authentication is the logon of section 1 and 3 of Fig. 11.1. Where the user logs on and provides a user name and password. The Kerberos server then authenticates the requestor. The local server only authenticates the ticket carried by the requestor to ensure that it is the correct ticket. In reference to the local server having the ability to permit or deny access to requests to secured items by requestors, for example in the absence of the central server. The applicant has not claimed this feature. The claim allows for the central server or the local server to perform the authentication. The system of Stallings discloses the central server performing the authentication therefore as, the claim is written, the local server is not required for any more authentication. As a result, the further authentication taught by Stallings is an addition.

The applicant argues further that Stallings does not teach that the Session keys limit a given requestor to accessing secure items using only a single one of the local servers or the central server such that the given requestor can only access secured items through at most one of the local servers at a time. This is not found persuasive. The ticket granted from the Kerberos server is once per user logon session, which provides a ticket for one service (Fig. 11.1). As a result, the access is limit. In order for serial access a new access ticket is required, just as in the parallel session, a new access is requested and therefore a new logon service and ticket and session key for the new access. The only difference between the serial session and the parallel session is that in the serial access, the access happens one after another, and in the parallel access the access happens within the same time period. It is, however, still true that a new access is required and as a result a new logon and new session key and ticket for the service (Fig. 11.1).

Even if, for the sake of argument, Stallings did not teach the limitation. The claim 36 does not claim preventing simultaneous (emphasis added) access to secured items. The claim recites, "wherein a given requestor, permitted to access secure items through one or more of said local servers, is only able to access secured items using only a single one of said local servers."

The applicant argued further that there is no motivation by a person of ordinary skill in the art implementing the system of Samson to restrict authentication to both a user and a client server, as it would defeat the flexibility in the system of Samson. This is not found persuasive. Boebert discloses a case when it would be desirable to curb the flexibility provided by Samson. In the case of departmental computing environments one may what want some users to have privileges that others do not have. This would reduce fraud, disruptive or erroneous directives, and sabotage (column 1 and column 2). The applicant argues further that Samson does not teach using an identification and authentication process for the user and the client machine. This taught by Boebert (column 4 lines 26-35). The applicant argues further that Samson does not teach retrieving access privileges associated with the user. This is true, however, Boebert teaches retrieving access privileges associated with the user (column 19 lines 4-15).

The examiner asserts that Samson and Boebert do teach or suggest the subject matter broadly recited in independent Claims 1, 21, 34-36. Dependent Claims 2-20, 22-33, and 37-44 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 1-44 are respectfully maintained.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 36 is rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for permitting access from any of the locations (Fig. 5F), does not reasonably provide enablement for "wherein a given requestor is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through at most one of said local servers at a time even though the given requestor is permitted to access secure items through more than one of said local servers". The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make the invention commensurate in scope with these claims. Questions are raised as to where control of the access is located, at the client or the server, so that the user can only access one server at a time. The disclosure (Fig. 5F) discloses gaining access to secure items from the first location, not the access of only a single one of local servers or the central server. The disclosure does not disclose that the system controls the number of servers that a user gains access, instead the disclosure discloses the control of the location that the user can access from. Is the access of only a single one of local server controlled by an Access control List, the location of the server, content of the server, encryption and key distribution? The examiner has assumed that the control of the number of servers accessed by the client is controlled by encryption and the distribution of keys for communication to a particular server.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 36 is rejected under 35 U.S.C. 102(b) as being anticipated by Stallings (Cryptography and Network Security).

In reference to claim 36, Stallings teaches the Keberos system comprising: a central server having a server module that provides overall access control (Keberos authentication server page 333); and a plurality of local servers, each of said servers including a local module that provides local access control (last paragraph on page 333), wherein the access control, performed by said central server or said local servers, operates to permit or deny access requests to secured items by requestors (Kerberos authentication server Fig 11.2), and wherein a given requestor is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through at most one of said local servers at a time even though the given requestor is permitted to access secure items through more than one of said local servers (page 336 Session keys).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Samson et al (6,339,423) in view of Boebert et al (5,502,766).

In reference to claims 1 and 34, Samson discloses a system and method comprising: (a) receiving, at a first server machine of the plurality of server machines (Fig. 2), an access request to access secure items from a user of a first client machine at a first location (column 4 lines 35-36), (b) authenticating the user of the first client machine at the first location (column 5 lines 30-45); (d) determining whether the user is permitted to gain access to secure items via the first location when said authenticating (b) and (c) are successful (column 4 line 62 to column 5 line 2) (e) permitting the user to gain access to secure items via the first server machine when said determining (d) determines that the user is permitted to gain access to secure items from the first location (Fig 3 A and B parts 318-338), and (f) preventing the user to gain access to secure items via the first server machine when said determining (e) determines that the user is not permitted to gain access to secure items from the first location (Fig 3A and B parts 318-332).

Although the system of Samson discloses and authentication process for the user, the system does not disclose (c) authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area.

In reference to claims 21 and 35, Samson discloses a system and method comprising: receiving, at a first server machine of the plurality of server machines (Fig. 2), an access request to access secure items from a user of a first client machine at a first location (column 4 lines 35-36), authenticating the user of the first client machine at the first location (column 5 lines 30-45); retrieving access privileges associated with the user (column 5 lines 38-46); determining whether the user is permitted to gain access to secure items via the first location when said authenticating are successful (column 4 line 62 to column 5 line 2) permitting the user to gain access to secure items via the first server machine when said determining determines that the user is permitted to gain access to secure items (Fig 3 A and B parts 318-338), and preventing the user to gain access to secure items via the first server machine when said determining determines that the user is not permitted to gain access to secure items from the first location (Fig 3A and B parts 318-332).

Although the system of Samson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claim 2, although the system of Samson discloses and authentication obtaining access privileges associated with the user (column 4 line 62 to column 5 line 2), Samson does not disclose a system of authentication wherein said determining comprises: to determine at least permitted locations for the user; and (d2) determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated with the user.

Boebert discloses a system for authentication wherein the determining comprises obtaining access privileges associated with the user to determine at least permitted locations for the user; and determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated wit the user (column 4 lines 27-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claim 3, wherein, when permitted by said permitting (e), the user gains access to secure items from the first location via the first client machine and the first server machine.

Although the system of Samson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access

engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claim 4, wherein, when permitted by said permitting (e), the user gains access to secure items from the first location via the first client machine and the first server machine.

Although the system of Samson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claims 5, 22, and 24, wherein said method comprises the acts of: (g) preventing the user from gaining access to secure items via any of the server machines other than the first server machine when said determining (d) determines that the user is permitted to gain access to secure items from the first location.

Although the system of Samson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35). The user is only permitted to access the resource from a particular location therefore since the other locations are not permitted to access the resource the no other server will permit access.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claims 6 and 23, wherein said determining (d) comprises determining whether the user is permitted to gain access to secure items via the first client machine and the first server machine, and wherein said permitting (e) operates to permit the user to gain access to secure items via the first client machine and the first server machine when said determining (d) determines that the user is permitted to gain access to secure items via both the first client machine and the first server machine.

Although the system of Samson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claim 7, wherein said determining comprises determining whether the user is permitted to gain access to secure items via the first server machine, and wherein said permitting operates to permit the user to gain access to secure items via the first server machine when said determining determines that the user is permitted to gain access to secure items via the first server machine (Fig 2 and 3).

In reference to claim 8, wherein said determining (d) comprises determining whether the user is permitted to gain access to secure items via the first client machine, and wherein said permitting (e) operates to permit the user to gain access to secure items via the first client

machine when said determining (d) determines that the user is permitted to gain access to secure items via the first client machine (Fig 2 and 3).

In reference to claim 9, wherein said method comprises the acts of: (g) preventing the user from gaining access to secure items via any of the server machines other than the first server machine when said determining (d) determines that the user is permitted to gain access to secure items from the first location.

Although the system of Samson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claims 10 and 25, wherein said preventing (g) of the user to gain access to secure items via any of the other server machines comprises reconfiguring at least any of the

other server machines that previously permitted the user to gain access to secure items therethrough.

Although Samson discloses preventing the user to gain access to secure items via any of the other server machines, Samson does not disclose preventing access to the server machine by reconfiguring at least any of the other server machines that previously permitted the user to gain access. Boebert also does not disclose the reconfiguration. However, Boebert discloses controlling access to the resource using keys.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to revoke the key from the user when the user is no longer permitted access in the system of Boebert. One of ordinary skill in the art would have been motivated to do this because when the user is no longer permitted to access the resource revoking the key would discourage fraudulent activities.

In reference to claims 11 and 26, wherein said permitting of the user to gain access to secure items via the first server machine comprises reconfiguring the first server machine to permit access by the user to secured items via the first server machine.

Although Samson discloses preventing the user to gain access to secure items via any of the other server machines, Samson does not disclose preventing access to the server machine by reconfiguring at least any of the other server machines that previously permitted the user to gain access. Boebert also does not disclose the reconfiguration. However, Boebert discloses controlling access to the resource using keys.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to revoke the key from the user when the user is no longer permitted access in the

system of Boebert. One of ordinary skill in the art would have been motivated to do this because when the user is no longer permitted to access the resource revoking the key would discourage fraudulent activities.

In reference claim 12 wherein said determining (d) comprises: obtaining access privileges associated with the user to determine at least permitted locations for the user; and determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated with the user.

Although the system of Samson discloses and authentication obtaining access privileges associated with the user (column 4 line 62 to column 5 line 2), Samson does not disclose a system of authentication wherein said determining comprises: to determine at least permitted locations for the user; and (d2) determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated with the user.

Boebert discloses a system for authentication wherein the determining comprises obtaining access privileges associated with the user to determine at least permitted locations for the user; and determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated wit the user (column 4 lines 27-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access

engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claims 13 and 27 wherein said permitting of the user to gain access to secure items via the first server machine comprises reconfiguring the first server machine to permit access by the user to secured items via the first server machine (column 5 lines 475-60).

In reference to claims 14 and 28 wherein each of the secure items is a secured file, the secured file having a format that comprises a header including security information as to who and how the secure item can be accessed, an encrypted data portion including data of the secure file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file.

Samson does not disclose an encrypted data portion. However Boebert discloses each of the secure items is a secured file, the secured file having a format that comprises a header including security information as to who and how the secure item can be accessed, an encrypted data portion including data of the secure file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file (Fig. 12).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access

engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claims 15 and 29, wherein the security information in the header of the secured file facilitates the restricted access to the secured file.

Boebert discloses a system wherein the security information in the header of the secured file facilitates the restricted access to the secured file (part 90 Fig. 8).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claim 16, wherein the security information in the header of the secured file points to or includes the access rules and a file key.

Boebert discloses the security information in the header of the secured file points to or includes the access rules and a file key (Fig. 10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access

engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claims 17 and 30, wherein the security information is encrypted with a user key associated with a user.

Boebert discloses the security information is encrypted with a user key associated with a user (Fig. 12).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claims 18 and 31, wherein the security information includes the file key and access rules to the restricted access to the secured file.

Boebert discloses security information includes the file key and access rules to the restricted access to the secured file (Fig. 16).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access

engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claims 19 and 32 wherein the file key is retrieved to decrypt the encrypted data portion in the secured file when access privilege of the user is within access permissions by the access rules.

Boebert discloses retrieving the file key to decrypt the encrypted data portion in the secured file when access privilege of the user is within access permissions by the access rules (Fig. 16).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Samson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to claims 20 and 33, wherein the access rules are expressed in a markup language. Samson and Boebert do not disclose the access rules are expressed in a markup language. However at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a markup language to express the access rules. One of ordinary skill in the art would have been motivated to do this because markup languages are a set of codes in a text file that instruct a computer how to format it on a printer or video display or how to

index and link its contents and therefore it would determine how to index the content based on the access rules.

Claims 37-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings as applied to claim 36 above, and further in view of Skarbo et al (6,317,777).

In reference to claim 37, wherein said access control system couples to an enterprise network to restrict access to secured files stored therein.

Stallings discloses the authentication to access to a service, however Stallings does not disclose access control system couples to an enterprise network to restrict access to secured files stored therein.

Skarbo discloses a document-collaboration videoconferencing system between na first and a second conference attendee (abstract). The system comprises access control system couples to an enterprise network to restrict access to secured files stored therein (Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art that the service provided by the server after authentication should be an enterprise network to restrict access to secured files stored therein as in the system taught by Skarbo in the server disclosed by Stallings. One of ordinary skill in the art would have been motivated to do this because the system would reliably deliver conferencing data to conference participants (Skarbo column1 lines 45-50).

In reference to claim 38, wherein the access requests are at least primarily processed in a distributed manner by said local servers (Fig. 11.2).

In reference to claim 39, wherein when the access requests are processed said local servers, the requestors gain access to the secured files without having to access said central server (Fig. 11.2).

In reference to claim 40, wherein the local module can be a copy of the server module so any of the local modules can operate independent of said central server and other of said local servers (Fig. 11.2).

In reference to claim 41, wherein the local module can be a subset of the server module (Fig. 11.2).

In reference to claim 42, wherein access permissions for said local servers can be dynamically configured to pass a requestor from one of said local servers to another of said local servers, thereby enabling access control to be performed by the another of said local servers such as when the location of the requestor changes (Fig. 11.2 multiple kerberi).

Claims 43-44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings and Boebert as applied to claim 37 above, and further in view of Pensak (6,449,721 B1).

In reference to claims 43-44, wherein the secured files are secured by encryption.

Although Stallings discloses the exchange of session keys, Stallings does not expressly disclose that the service is secured by encryption.

Pensak discloses secured files are secured by encryption (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to secure the files by encryption as in Pensak in the system of Stallings. One of

ordinary skill in the art would have been motivated to do this because encryption is a process for encoding data that prevents unauthorized access especially during transmission.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Thursday, June 22, 2006

HOSUK SONG
PRIMARY EXAMINER